TRƯỜNG ĐẠI HỌC CÔNG THƯƠNG
THÀNH PHỐ HỒ CHÍ MINH
KHOA CÔNG NGHỆ THÔNG TIN

DANH SÁCH KHÓA LUẬN CỬ NHÂN NGÀNH ATTT HỌC KỲ 2 NĂM HỌC 2025 - 2026

STT ĐỀ TÀI	TÊN ĐỀ TÀI	NỘI DUNG YÊU CẦU	GIÁO VIÊN HƯỚNG DẪN	EMAIL	BỘ MÔN	Định hướng đề tài (Ứng dụng, Nghiên cứu, Kết hợp, MMT)	GHI CHÚ
1	Xây dựng hệ thống quản lý học tập tích hợp tính năng phát hiện và nhận diện khuôn mặt (FaceID) để quản lý lớp học	- Nghiên cứu các các hệ thống quản lý học tập thực tế - Nghiên cứu các công nghệ: OpenCV, Yolo, Canvas… - Thiết kế hệ thống LMS gồm các tính năng: + Quản lý giảng viên: hồ sơ giảng viên (cơ hữu và thỉnh giảng), lịch dạy, lớp dạy, v.v… + Quản lý sinh viên: hồ sơ sinh viên, lịch học, điểm số,.v… +Quản lý lớp học: Tạo lớp học, điểm danh, phân nhóm, kiểm tra, điểm số, xuất danh sách điểm danh, v.v… - Thiết kế tính năng FaceID và tích hợp vào hệ thống LMS: + Xử lý hình ảnh đầu vào từ camera để phục vụ cho các bước phân tích (computer vision) + Xây dựng tính năng phát hiện khuôn mặt từ camera (object detection).	Lê Tỳ Khánh, Vũ Đức Thịnh	thinhvd@huit.edu.vn	MMT&ATTT	Ứng dụng	
2	Nghiên cứu về deepfake và các giải pháp phòng chống	- Nghiên cứu các kỹ thuật Deepfake - Nghiên cứu các công cụ: Voice Cloning, AI voice synthesis, Microsoft Video Authenticator, Deepware Scanner - Nghiên cứu và phân tích công nghệ giả mạo giọng nói: + Phân tích Voice Cloning, AI voice synthesis + Xác định dấu hiệu nhận diện Deepfake voice: ngữ điệu, âm thanh nền, độ khớp nội dung + Xác định các biện pháp phòng chống: xác thực đa yếu tố, xác minh qua kênh song song, voice biometrics - Nghiên cứu và phân tích các công cụ deepfake video + Phân tích Microsoft Video Authenticator, Deepware Scanner + Xác định dấu hiệu nhận diện Deepfake video + Xác định các biện pháp phòng chống deepfake vieo	Lê Tỳ Khánh, Vũ Đức Thịnh	thinhvd@huit.edu.vn	MMT&ATTT	Nghiên cứu	
3	Ứng dụng kỹ thuật học sâu trong phát hiện tấn công ứng dụng web	-Nghiên cứu các phương pháp tân công ứng dụng web như: URLs detect, HTTP traffic, SSRF, command injection v.v... - Nghiên cứu các kỹ thuật học sâu như: CNN, LSTM, Bi-LSTM, RNN, Auto-encoder v.v.. - Ứng dụng một kĩ thuật học sâu hoặc kết hợp vào phát hiện bất thường dịch vụ web - Triển khai mô hình huấn luyện, thực nghiệm các trên real-world datasets - So sánh, biện luận kết quả với các phương pháp SOTA khác - Viết ứng dụng minh họa	Phạm Văn Phùng, Phạm Nguyễn Huy Phương	phuongpnh@huit.edu.	MMT&ATTT	Nghiên cứu	
4	Nghiên cứu mô hình học sâu Bi-LSTM kết hợp Word Embedding ứng dụng trong phát hiện Email lừa đảo	- Phân tích các đặc trưng của email lừa đảo (Domain giả mạo, từ khoá đáng ngờ, liên kết độc hại). - Thu thập và tiền xử lý tập dữ liệu email từ các nguồn công khai như SpamAssassin, Enron Corpus, Kaggle, v.v. - Biểu diễn văn bản email thành dạng vector ngữ nghĩa sử dụng kỹ thuật Word Embedding (Word2Vec hoặc GloVe). - Xây dựng và huấn luyện mô hình học sâu Bi- LSTM để nhận diện email lừa đảo dựa trên dữ liệu văn bản.	Nguyễn Thị Hồng Thảo	thaonth@huit.edu.vn	MMT&ATTT	Nghiên cứu	

5	Xây dựng hệ thống xác thực đa nhân tố (OTP) cho website	-Tìm hiểu về cơ chế xác thực đăng nhập, - Phân loại và phân tích chi tiết các cơ chế xác thực phổ biến (một yếu tố, hai yếu tố, đa yếu tố). - Tìm hiểu về phương pháp sinh mã (HOTP , TOTP) - Xây dựng hệ thống xác thực 2 lớp (Xây dựng website, ứng dụng đọc mã OTP/ QR, xác thực tin nhắn bằng Email/ Điện thoại di động	Trần Thị Bích Vân	vanttb@huit.edu.vn	MMT&ATTT	Ứng dụng	
6	Xây dựng tập dữ liệu WiFi Fingerprinting có bảo vệ quyền riêng tư bằng Differential Privacy	MỤC TIÊU: - Đề xuất cơ chế Differential Privacy (DP) có xét đến mức độ quan trọng của AP. - Giảm thiểu sai số định vị so với DP chuẩn. - Phân tích so sánh trên dataset đã công bố. - Đánh giá khả năng công bố dữ liệu an toàn. YÊU CẦU: + Tổng quan về đề tài: Hiện nay, nhiều bộ dữ liệu WiFi Fingerprinting đã được xây dựng phục vụ cho việc nghiên cứu các hệ thống định vị trong nhà. Tuy nhiên, ngay cả khi dữ liệu đã được ẩn danh, vẫn tồn tại nguy cơ thông tin vị trí người dùng bị lộ và phục vụ mục đích không tốt. Do đó, việc áp dụng Differential Privacy để bảo vệ tập dữ liệu WiFi Fingerprinting là cần thiết, đồng thời phải đảm bảo dữ liệu vẫn hữu ích cho bài toán định vị. + Tìm hiểu thuật toán áp dụng cho bài toán: Xây dựng phương pháp tạo tập dữ liệu ngoại tuyến WiFi Fingerprinting có bảo vệ quyền riêng tư bằng Differential Privacy, đồng thời tối ưu hóa độ chính xác của các mô hình định vị được huấn luyện trên dữ liệu đó. + Cài đặt thuật toán: Differential Privacy cho fingerprint DB; + Đánh giá kết quả thực nghiệm: so sánh kết quả định vị với dữ liệu gốc. + Các chỉ số đánh giá: Sai số định vị, accuracy loss, privacy budget NNLT: Python.	Nguyễn Hữu Khánh	khanhnh@huit.edu.vn	MMT&ATTT	Nghiên cứu	
7	Định vị trong nhà dựa trên WiFi Fingerprinting có bảo vệ quyền riêng tư người dùng bằng Differential Privacy	MỤC TIÊU: - Phân tích ảnh hưởng của Differential Privacy lên độ chính xác định vị. - Đề xuất cơ chế DP thích nghi theo độ ổn định của RSSI. - So sánh kết qủa định vị trước và sau cải tiến. - Đánh giá khả năng bảo vệ quyền riêng tư người dùng. YÊU CẦU: + Tổng quan về đề tài: Định vị trong nhà dựa trên kỹ thuật WiFi Fingerprinting là một trong những phương pháp phổ biến do khả năng tận dụng được hạ tầng WiFi sẵn có. Tuy nhiên, dữ liệu WiFi fingerprint (RSSI) kết hợp với thông tin vị trí là dữ liệu nhạy cảm, có thể bị khai thác để theo dõi người dùng một ca1hc bất hợp pháp. Do đó, để bảo vệ quyền riêng tư của người dùng, việc tích hợp Differential Privacy (DP) trong quá trình định vị là một hướng nghiên cứu cần thiết, có ý nghĩa khoa học và thực tiễn. + Tìm hiểu thuật toán áp dụng cho bài toán: Xây dựng mô hình định vị trong nhà dựa trên WiFi Fingerprinting, trong đó dữ liệu RSSI của người dùng được bảo vệ bằng Differential Privacy trước khi sử dụng cho bài toán định vị. + Cài đặt thuật toán: Áp dụng Local Differential Privacy trực tiếp lên RSSI của người dùng trong pha định vị trực tuyến; + Đánh giá kết quả thực nghiệm: so sánh kết quả định vị trước và sau khi cải tiến. + Các chỉ số đánh giá: Sai số định vị, accuracy loss, privacy budget NNLT: Python	Dương Bảo Ninh	ninhdb@huit.edu.vn	MMT&ATTT	Nghiên cứu	

8	Nghiên cứu về Visual-Audio Anti-Spoofing trong môi trường thực: Học đặc trưng bất biến miền và thích nghi few-shot	Mục tiêu: Xây dựng hệ Audio-Visual PAD (Face+Voice) phát hiện real/spoof tổng quát hóa tốt khi đổi dataset/thiết bị và có thể thích nghi few-shot với miền mới. Dữ liệu: Video mặt + audio đồng bộ; benchmark cross-dataset/cross-device và k-shot (1/5/10). Đánh giá bằng EER, APCER/BPCER, AUC, so sánh Face-only / Voice-only / Fusion. Phương pháp: ResNet-18/MobileNetV3 hoặc ViT cho face, ECAPA-TDNN hoặc wav2vec 2.0 cho voice; fusion bằng late fusion hoặc Cross-Attention Transformer. Học domain-invariant với DANN/Gradient Reversal, học biểu diễn bằng contrastive (InfoNCE/CLIP-style), và few-shot bằng Prototypical Networks (hoặc MAML-lite). Triển khai bằng PyTorch, tiền xử lý mặt với MediaPipe/RetinaFace, audio với log-mel/MFCC. Link file kế hoạch thực hiện: https://docs.google.com/document/d/1T9uNTGZGUOVIMvQgGP45Rn08l0cGml57GuolDf7Xf5o/edit?usp=sharing	Đỗ Minh Tiến	tiendm@huit.edu.vn	MMT&ATTT	Nghiên cứu	
9	Xây dựng hệ thống quản lý học tập tích hợp chữ ký số để quản lý hồ sơ	- Nghiên cứu, phân tích thiết kế các tính năng, xây dựng hệ thống quản lý học tập: + Quản lý giảng viên: hồ sơ giảng viên (cơ hữu và thỉnh giảng), lịch dạy, lớp dạy, v.v… + Quản lý sinh viên: hồ sơ sinh viên, lịch học, điểm số… + Quản lý lớp học: Tạo lớp học, điểm danh, phân nhóm, kiểm tra, điểm số, xuất danh sách điểm danh, v.v… - Xây dựng tính năng chữ ký số và tích hợp vào hệ thống quản lý học tập + Nghiên cứu về các hệ ký số RSA, DSS, DSA... + Xây dựng tính năng ký số trên các văn bản tích hợp vào hệ thống quản lý học tập	Phạm Văn Phùng, Vũ Đức Thịnh	thinhvd@huit.edu.vn	MMT&ATTT	Ứng dụng	
10	Nghiên cứu phát hiện tấn công xen giữa (Man-in-the-Middle) qua phân tích chứng chỉ số	Nghiên cứu cơ chế hoạt động của giao thức SSL/TLS và cấu trúc chứng chỉ số X.509. Xây dựng công cụ có khả năng giám sát, phân tích các đặc trưng của chứng chỉ (Fingerprint, Issuer, Chain of Trust) để phát hiện và cảnh báo các cuộc tấn công Man-in-the-Middle (MitM) trong thời gian thực. - Nghiên cứu kiến trúc hạ tầng khóa công khai (PKI), chuẩn X.509 và quy trình bắt tay (Handshake) của TLS 1.2/1.3. - Phân tích kỹ thuật tấn công MitM (SSL Stripping, Fake CA) và cách các công cụ như mitmproxy, Ettercap tạo chứng chỉ giả. - Thiết kế thuật toán phân tích sâu (Deep Inspection) dựa trên so sánh Fingerprint và kiểm tra sự thay đổi bất thường của Issuer (Anomalies Detection) thay vì chỉ kiểm tra chữ ký số đơn thuần. - Xây dựng môi trường giả lập (Attacker, Victim, Gateway) để thu thập mẫu dữ liệu chứng chỉ "sạch" và "độc". - Xây dựng Script bắt gói tin, trích xuất thông tin chứng chỉ và cảnh báo khi có dấu hiệu giả mạo trên ngôn ngữ Python (thư viện Scapy/OpenSSL). - Đánh giá độ chính xác (Detection Rate) và khả năng giảm thiểu cảnh báo giả (False Positive) của công cụ.	Đinh Huy Hoàng	hoangdhuy@huit.edu.	MMT&ATTT	Nghiên cứu	

11	Nghiên cứu và triển khai các giải thuật băm mật khẩu hiện đại (Bcrypt, Scrypt, Argon2) trong hệ thống xác thực.	-Nghiên cứu các khái niệm về Salt, Pepper, Work Factor và cơ chế chống tấn công bảng băm (Rainbow Table). -Phân tích sự khác biệt về kỹ thuật giữa Bcrypt (CPU intensive), Scrypt (Memory intensive) và Argon2 (Memory-hard). -Thiết kế mô hình thử nghiệm so sánh tốc độ băm và khả năng chiếm dụng tài nguyên hệ thống (CPU/RAM). -Xây dựng môi trường giả lập sử dụng các công cụ như Hashcat hoặc John the Ripper để kiểm tra độ bền của mật khẩu đã băm. -Lập trình ứng dụng Web/API bằng Python (sử dụng thư viện passlib hoặc argon2-cffi) để tích hợp và kiểm thử các giải thuật. -Đánh giá và đưa ra khuyến nghị sử dụng giải thuật phù hợp dựa trên các tiêu chuẩn bảo mật hiện hành.	Lê Anh Tuấn	tuanla@huit.edu.vn	MMT&ATTT	Nghiên cứu	

NGƯỜI LẬP

Lương Thị Quỳnh Mai

KT. TRƯỞNG KHOA
PHÓ TRƯỞNG KHOA

Nguyễn Thị Bích Ngân